Tema 3: Modelos de gestión de red

1. SNMP.
2. OSI.

SNMP

Historia

- Desde el origen de TCP/IP(1969) se utiliza para gestión herramientas basadas en el protocolo ICMP (Internet-Control Message Protocol) .
- La principal herramienta es PING (Packet INternet Groper), que permite comprobar la comunicación entre dos máquinas, calcular tiempos medios de respuesta y pérdidas de paquetes.
- Al ser parte de la familia de protocolos TCP/IP, todas las máquinas disponen de este protocolo.

- Con el crecimiento exponencial de Internet a partir de los años 80, surge la necesidad de herramientas estándar de gestión más potentes.

Historia

- En los años 80 surgen tres propuestas de estándar de protocolo de gestión para TCP/IP:
  - **HEMS** (High-level entity-management system), que es una generalización del que fue quizás el primer protocolo de gestión usado en Internet (HMP)
  - **SNMP** (Simple network management protocol), que es una versión mejorada de SGMP (Simple gateway-monitoring protocol)
  - **CMOT** (CMIP over TCP/IP), que intenta incorporar, hasta donde sea posible, el protocolo (common management information protocol), servicios y estructura de base de dato que se están estandarizando por ISO
- A principios de 1988, el **IAB** recibe las propuestas y decide el desarrollo de SNMP como solución a corto plazo y CMOT a largo plazo (ya que supone que con el tiempo las redes TCP/IP evolucionarán a redes OSI). HEMS es más potente que SNMP, pero como se supone que se va a producir la transición a OSI, se elige SNMP por ser más simple y necesitar menos esfuerzo para desarrollarse (ya que se supone que va a desaparecer con el tiempo).

Historia

- SNMP se estandariza en los años 90/91, y aunque era una solución simple a corto plazo, el retraso en la aparición de redes OSI y la gran cantidad de redes TCP/IP, le augura una larga vida, mientras que los trabajos en CMOT se ralentizan.

- Actualmente es un estándar utilizado universalmente y se está ampliando a todo tipo de redes (no sólo TCP/IP) incluido OSI.

- Durante su historia ha ido evolucionado desde el estándar simple original. Las principales extensiones aumentan su funcionalidad y cubren problemas de seguridad detectados en el protocolo original.

Evoluciones más importantes

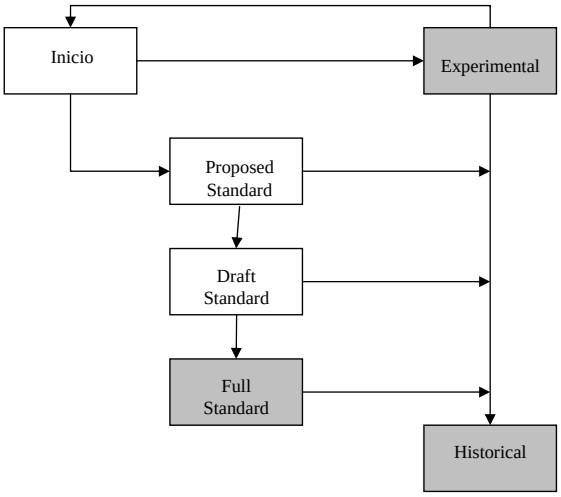
- Extensiones de la MIB:
  - **RMON** (remote-monitoring), que permite monitorizar subredes como un todo, además de equipos individuales. Aunque es reciente, ya es ampliamente utilizado.
  - Otras extensiones:
    - Independientes de vendedores: principalmente para soportar interfaces de red como Token-Ring o FDDI
    - Dependientes del vendedor para soportar características específicas de sus productos.
- Otras extensiones:
  - De funcionalidad
  - De seguridad

Evoluciones más importantes

- Extensiones de seguridad y funcionalidad:
  - En Julio de 1992 se proponen 3 documentos. No son compatibles con SNMP original ya que cambia el formato de las cabeceras aunque no las PDU (packet data unit) contenidas en los mensajes, ni el número de PDUs
  - También en Julio de 1992, cuatro organismos proponen una extensión de SNMP llamada SMP (Simple Management Protocol). Al mismo tiempo aparecen 4 implementaciones (dos comerciales y dos públicas). SMP añade tanto nuevas funcionalidades como mejoras de seguridad, por tanto añade nuevas PDUs y los cambios de cabeceras comentados antes.
  - El IETF acepta SMP como base para la versión 2 de SNMP (SNMPv2), creandose dos grupos de trabajo, uno centrado en la seguridad y otro en los demás aspectos.
  - El resultado fueron 12 documentos publicados como *proposed standards* a principios de 1993. Aunque no son estándares finales ya son soportados por multitud de fabricantes.

Estándares en Internet

- Los estándares son publicados por el IAB (Internet Activities Board) a propuesta del IETF (Internet Enginnering Task Force). (El IAB tiene otro grupo denominado IRTF- Internet Research Task Force) como RFCs y Estándares Finales.



Estándares de SNMP

- 3 ***Full Standards***:
  - RFC 1155(STD 16): Estructura e identificación de la información de gestión para Internets basadas en TCP/IP. Mayo de 1990.
    - Define como se definen en la MIB los objetos gestionados.
  - RFC 1157 (STD 15): A Simple Network Management Protocol (SNMP). Mayo de 1990.
    - Define el protocolo para gestionar los objetos.
  - RFC 1213 (STD 17): Management Information Base para gestión de red en Internets basadas en TCP/IP:Ñ MIB-II. Marzo de 1991
    - describe los objetos almacenados en la MIB.
- 1 ***Draft Standard***
- 20 ***Proposed Standards***
- 4 ***Experimental Standards***: entre ellos SNMP sobre OSI
- 2 ***Informational***

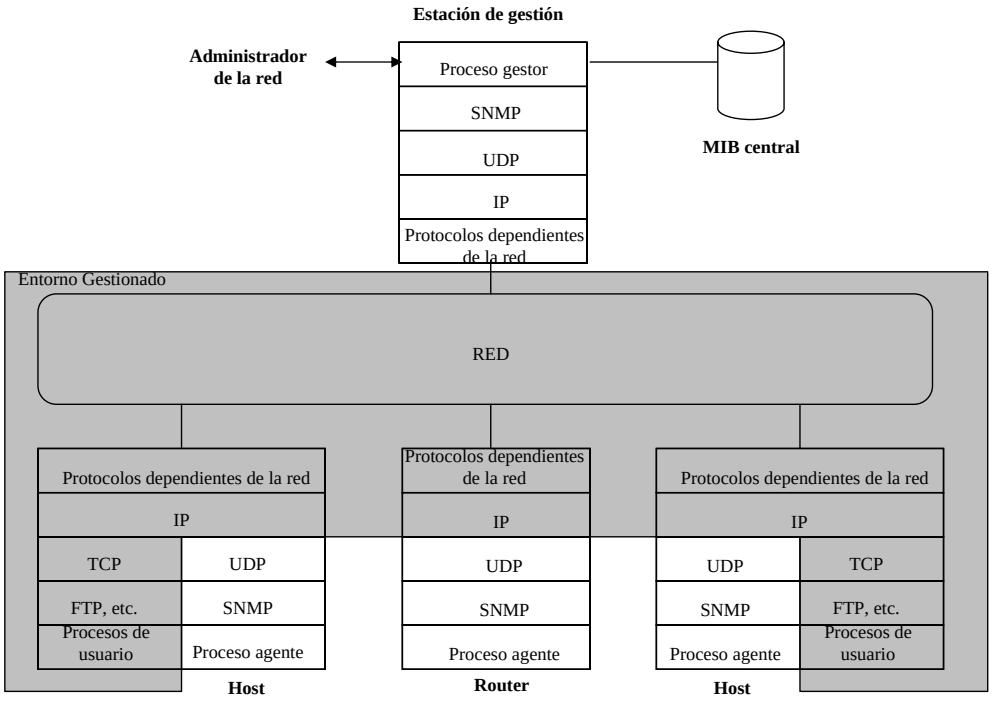
Arquitectura

- Estructura clásica ya vista:
  - Estación de gestión
  - Agentes de gestión (incluidos agentes *proxy*)
  - Base de información de gestión (MIB)
  - Protocolo de gestión de red
- De los elementos de la estación de gestión: aplicaciones (para análisis de datos, etc.), intefaz de usuario, capacidad de convertir las solicitudes del usuario apeticiones demonitorización y control a los elementos remotos y base de datos con información de las MIBS de los elementos de la red gestionados, sólo los dos últimos son cubieros por SNMP.
- Los agentes mantendrán una MIB local, atenderán solicitudes de la estación de gestión y podrán enviar de manera asíncrona informes de eventos importantes (*event reporting*). Soporta por tanto los dos mecanismos de comunicación agente-gestor que conocemos.

Arquitectura

- La MIB local de cada agente mantiene información sobre objetos del recurso que gestiona almacenada en forma de pares atributo-valor. Los objetos están estandarizados para recursos del mismo tipo (p.e., todos los concentradores tendrán los mismos objetos).
- El protocolo (SNMP) enlaza la estación de gestión y los agentes. El protocolo es muy simple, proporcionando las siguientes posibilidades:
  - ***Get***: permite a la estación gestora obtener valores de objetos de agentes.
  - ***Set***: permite a la estación gestora modificar valores de objetos de agentes.
  - ***Trap***: permite a un agente enviar de manera asíncrona la notificación de un evento importante a la estación de gestión.
- En el estándar no se indica nada acerca del número de estaciones gestoras o del ratio gestores/agentes, aunque lo normal es tener dos estaciones gestoras (una de *backup*) y al ser el protocolo simple, el número de agentes por gestor puede ser bastante alto (centenares).

Entorno de gestión



MIB

- Almacena una serie de valores relacionados con los elementos gestionados. Cada recurso gestionado se representa por un **objeto**.
- Independientemente del protocolo, una MIB debe cumplir:
  - El objeto u objetos usados para representar un recurso concreto deben ser los mismos en cada nodo (p.e., el número de conexiones TCP abiertas durante un período de tiempo está formado por sesione activas y pasivas. Guardando dos de los tres posibles valores (sesiones activas, pasivas o totales) podemos obtener el tercero. Pero si almacenamos en cada nodo dos distintos, es difícil diseñar un protocolo simple para acceder a esa información).
  - Se debe utilizar un esquema común de representación de la información para permitir la interoperatividad. Esto se consigue en SNMP mediante la definición SMI (structure of management información) (RFC 1155).

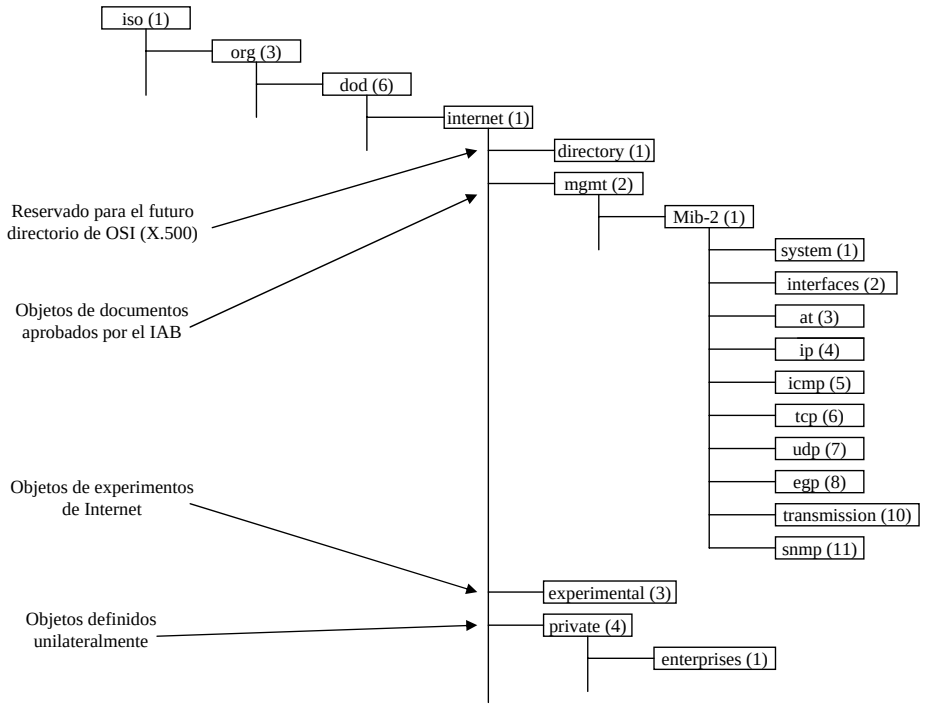
Estructura de la MIB (SMI)

- Identifica los tipos de datos que se pueden utilizar y cómo los recursos se representan y nombran en la MIB.
- La filosofía de SMI es:
  - **Simplicidad**: sólo tipos de datos simples: escalares y arrays de dos dimensiones de escalares. El protocolo sólo puede acceder a escalares, incluyendo elementos individuales de una tabla.
  - **Posibilidad de extensión**: para poder introducir nuevos objetos, dependientes o independientes del fabricante. La introducción de objetos dependientes del fabricante afectará a la interoperatividad.
- El SMI define:
  - La estructura de la MIB (en ASN.1).
  - Sintaxis y tipos de valores para objetos individuales (en ASN.1).
  - Codificación de los valores de los objetos (en ASN.1).

Estructura de la MIB (SMI)

- La describiremos sin entrar en profundidad en la definición en ASN.1
- Cada tipo concreto de objeto tiene un identificador único que sirve para nombrarlo. Además como el valor asociado a cada identificador es jerárquico (una secuencia de enteros), dichos identificadores también definen la estructura de la MIB (es una estructura en forma de árbol).
- Empezando por la raíz, existen tres nodos de primer nivel: **iso**, **ccitt** y **join-iso-ccitt**.Como ejemplo, bajo **iso**, un subárbol se reserva para uso de otras organizaciones, y una de ellas es el departamento de defensa de EEUU (**dod**). El RFC 1155 reserva un subárbol de **dod** para la Internet Activities Board (IAB) de la siguiente manera:
  - internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
- Es decir, el nodo **internet** tiene el valor de identificador de objeto **1.3.6.1**, que valdrá como prefijo para nodos a niveles más bajos del árbol

Estructura de la MIB (SMI)



Estructura de la MIB (SMI)

- El **mgmt** contiene definiciones de información aprobada por el IAB. Actualmente existen dos versiones de la MIB: **mib-1** y **mib-2**. La segunda es una extensión de la primera. Como tienen el mismo identificador sólo uno puede estar presente.
- Se pueden definir objetos adicionales en la MIB de tres maneras:
  - Expandiendo la **mib-2** (por ejemplo se ha introducido RMON) o reemplazandola por una nueva (futura mib-3).
  - Construyendo una MIB experimental para una aplicación que después puede pasar al subárbol **mgmt** (p.e., MIBs de varios medios de transmisión que se han definido, como token-ring (RFC 1231), etc.)
  - Extensiones privadas en el subárbol **private**. Por ejemplo el RFC 1227 define el MUX (para multiplexores)
- El objeto **private** actualmente sólo tiene un subárbol (**enterprises**) donde los fabricantes pueden almacenar extensiones propias. Cada fabricante registrado tiene su propio subárbol bajo **enterprises**.

Estructura de la MIB (SMI)

- Sintaxis y tipos de valores para objetos individuales:
  - Se definen como tipos de ASN.1.
  - Sólo se pueden utilizar los tipos universales más simples de ASN.1 y algunos definidos.
- Codificación de los valores de los objetos:
  - Se utilizan las reglas básicas de ASN.1 (**BER** - basic encoding rules).
  - No son las reglas más compactas o eficientes posibles pero es un esquema estandarizado y ampliamente utilizado.

Contenidos de la MIB

- La **MIB-II** (RFC 1213) es la segunda versión estandarizada. Es un superconjunto de la **MIB-I** (RFC 1156) con objetos y grupos adicionales
- Criterios especificados en la RFC para incluir un objeto en la MIB-II:
  - Ser esencial para la gestión de configuración o fallos
  - Sólo se permiten objetos cuya modificación provoque daños limitados (refleja la falta de mecanismos de seguridad en SNMP)
  - Tiene uso actual y utilidad
  - MIB-I intentaba mantener los objetos por debajo de 100, en MIB-II se elimina ese límite ya que cada vez hay mas tecnologías que gestionar
  - No es redundante. Se eliminan todos los que se pueden derivar de otros
  - Se eliminan objetos dependientes de implementaciones concretas (p.e., para BSD UNIX)
  - Se minimizan las secciones críticas de código

Contenidos de la MIB

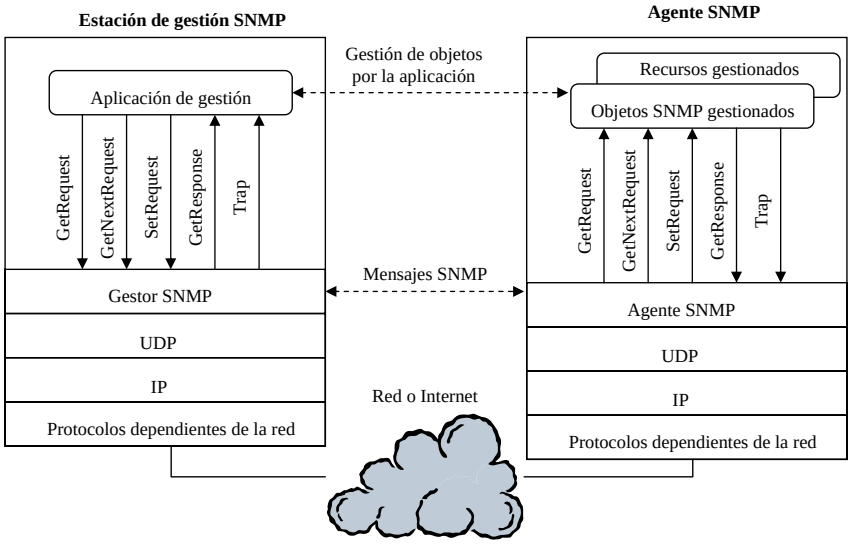
- Hay 10 grupos:
  - **system**: información general del sistema (7 objetos)
  - **interfaces**: “ de cada uno de los interfaces de red (2 subárboles: 1 y 22 obj.)
  - **at** (address-translation, despreciado): mapeo internet-subred (3 obj.)
  - **ip**: información sobre el protocolo IP (60 objetos con 4 subárboles)
  - **icmp**: 26 objetos
  - **tcp**: 18 objetos y 2 subárboles
  - **udp**: 6 objetos y 2 subárboles
  - **egp**: 20 objetos y 2 subárboles
  - **transmission**: información sobre los esquemas de transmisión y protocolos de acceso (el número de objetos es variable)
  - **snmp**: 30 objetos.

Protocolo SNMP

- El protocolo (SNMP) enlaza la estación de gestión y los agentes. El protocolo es muy simple, proporcionando las siguientes posibilidades:
  - ***Get***: permite a la estación gestora obtener valores de objetos de agentes.
  - ***Set***: permite a la estación gestora modificar valores de objetos de agentes.
  - ***Trap***: permite a un agente enviar de manera asíncrona la notificación de un evento importante a la estación de gestión.
- No permite modificar la estructura de la MIB añadiendo o eliminando objetos. Por tanto sólo permite acceder a las hojas del árbol.
- Tampoco permite comandos para realizar acciones.
- La seguridad se hace mediante comunidades (un nombre con un conjunto de operaciones permitidas) definidas en los agentes (un agente puede tener varias comunidades definidas). El nombre va en las peticiones y es el único mecanismo de autentificación soportado (seguridad casi nula).
- Estas características hace simple el protocolo, pero limitan las posibilidades de gestión.
- No vamos a ver la especificación de las 5 primitivas definidas.

Protocolo

- El protocolo es un protocolo de nivel de aplicación de tipo datagrama (UDP), por tanto no existe sesión, cada intercambio es una transacción independiente entre el gestor y el agente.



Limitaciones de SNMP

- El protocolo no es muy adecuado para leer grandes cantidades de datos (como tablas de encaminamiento).
- No hay asentimiento de las *Traps*, no sabiendo el agente si ha llegado a la estación gestora.
- Mecanismo trivial de autentificación.
- No soporta comando imperativos directos. Se puede hacer indirectamente modificando un valor que implique una acción (más limitado que comandos directos).
- El modelo de la MIB es limitado y no soporta operaciones complejas como consultas basadas en valores o tipos de objetos.
- No soporta comunicaciones gestor-gestor, de tal manera que por ejemplo una máquina gestora no puede obtener información sobre dispositivos o redes de otras máquinas gestoras.

- Como ya dijimos, algunas de estas limitaciones se han mejorado con extensiones como RMON o SNMPv2.

SNMPv2

- No lo vamos a ver.
- Mejora SNMP en:
  - Estructura de la Información gestionada (SMI)
  - Primitivas del protocolo
  - Capacidad de comunicación gestor a gestor
  - Seguridad
- Las dos primeras permiten la definición y acceso a tipos de datos complejos no soportados por SNMP. También permite un acceso más eficiente a los datos (tablas, etc.) que sí soportaba SNMP.
- En seguridad se introduce cifrado con clave pública y firma digital.

OSI

Introducción

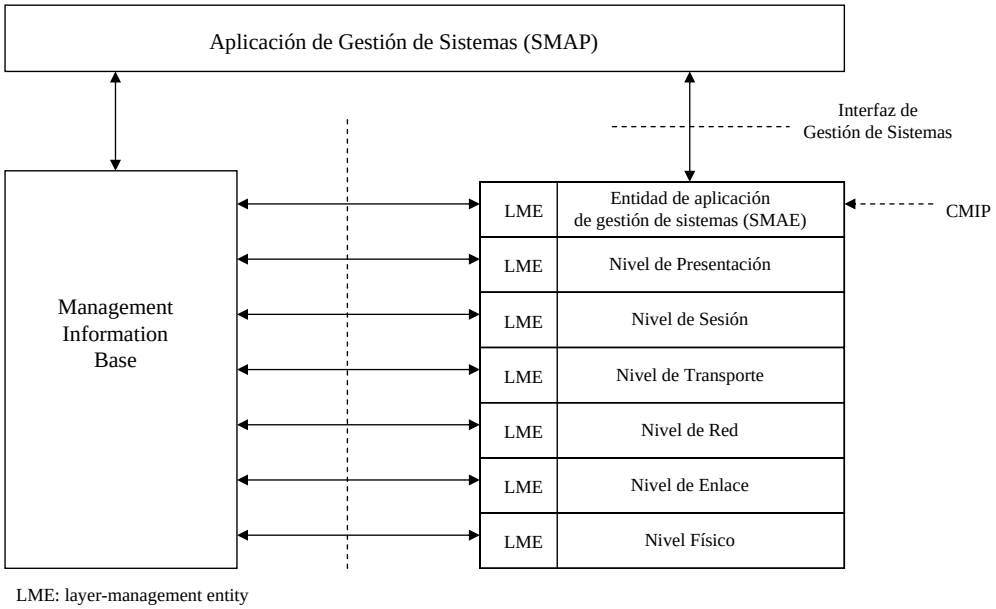
- Conjunto de muchos estándares (es el más amplio y complejo de todos los desarrollados por ISO) desarrollados conjuntamente por ISO y CCITT para gestión de redes OSI.
- CCITT tiene reservada la serie de números X.700 para este conjunto de estándares.
- El conjunto de estándares se denomina **Gestión de sistemas OSI** (***OSI systems management***) e incluye la definición de:
  - Un servicio de gestión (CMIS - Common Management Information Service).
  - Un protocolo de gestión (CMIP - Common Management Information Protocol).
  - Una base de datos.
  - Otros conceptos relacionados.
- En OSI se utiliza el término **gestión de sistemas** en vez de gestión de red.

Estándares

- Actualmente existen 37 estándares.
- El primero fue el ISO 7498-4 (X.700) que especifica el entorno de gestión para el modelo OSI (introducción general a los conceptos básicos de gestión: arquitectura, terminología utilizada, etc.).
- Los podemos agrupar en los siguientes apartados:
  - **Entorno de gestión e Introducción** (2documentos): El ISO 7498-4, y el ISO 10040 (X.701) que introduce y describe los demás documentos.
  - **CMIS/CMIP** (6 documentos): especifican el CMIS que proporciona servicios a las aplicaciones de gestión y el CMIP que soporta el CMIS.
  - **Funciones de gestión** (22 documentos): especifican las funciones específicas que se definen para el sistema de gestión OSI.
  - **Modelo de información de gestión** (5 documentos): especifica la MIB.
  - **Gestión de niveles OSI** (2 documentos): especifican información, servicios y funciones relacionadas con niveles específicos de la torre OSI.

Modelo de arquitectura (CMIS)

- Un equipo gestionado dentro del entorno OSI seguirá el siguiente modelo de arquitectura:

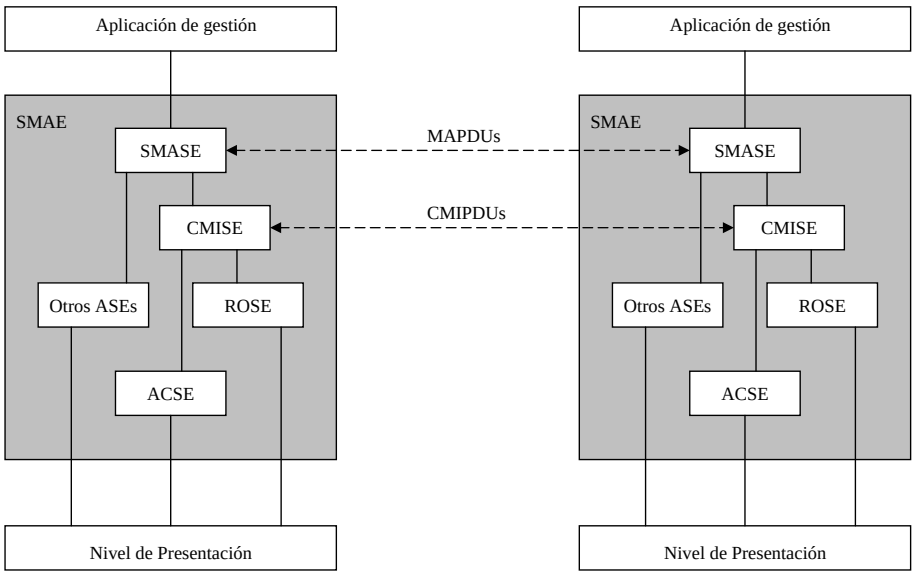


LME: layer-management entity

Modelo de arquitectura (CMIS)

- Los elementos clave de este modelo de arquitectura son:
  - **Aplicación de gestión de sistemas (SMAP - *systems-management application process*)**: Software local de un equipo (sistema) gestionado que implementa las **funciones de gestión** para ese sistema (host, router, etc.). Tiene acceso a los parámetros del sistema y puede, por tanto, gestionar todos los aspectos del sistema y coordinarse con SMAPs de otros sistemas.
  - **Entidad de aplicación de gestión de sistemas (SMAE - *systems-management application entity*)**: Entidad de nivel de aplicación responsable del intercambio de información de gestión con SMAEs de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red. Para esta función se utiliza un protocolo normalizado (CMIP)
  - **Entidad de gestión de nivel (LME - *layer-management entity*)**: Proporciona funciones de gestión específicas de cada capa de la torre OSI.
  - **Base de información de gestión (MIB)**.

Estructura de la entidad SMAE



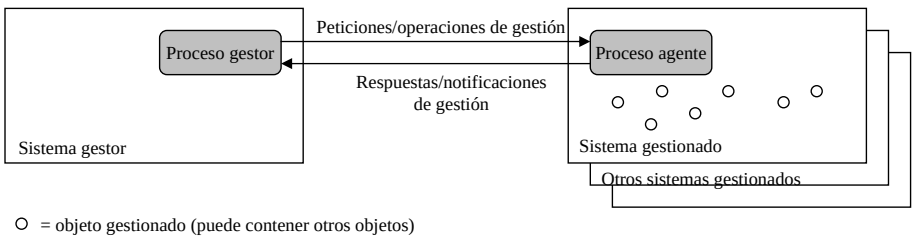
MAPDU = management-application protocol data unit.
CMIPDU = common management-information protocolo data unit.

Estructura de la entidad SMAE

- Como cualquier entidad de nivel de aplicación se define a nivel lógico como un conjunto de elementos de servicio de aplicación (**ASE - *application-service element***). En concreto en la figura destacamos cuatro:
  - De propósito general (diseñadas para ser útiles en muchas aplicaciones):
    - **ACSE (*association-control-service element*).**
    - **ROSE (*remote-operations-service element*).**
  - Específicas para gestión de sistemas:
    - **SMASE (*system-management application-service element*)**: implementa funciones básicas de gestión en las áreas de gestión de fallos, costes, configuración, prestaciones y seguridad. Proporciona servicios al gestor de red y a las aplicaciones de gestión (p.e., SMAP).
    - **CMISE (*common management information service element*)**: proporciona funciones básicas de gestión que soportan las 5 áreas funcionales. EL SMASE delega en este elemento aquellas funciones que requieren comunicación con otros sistemas.

Arquitectura

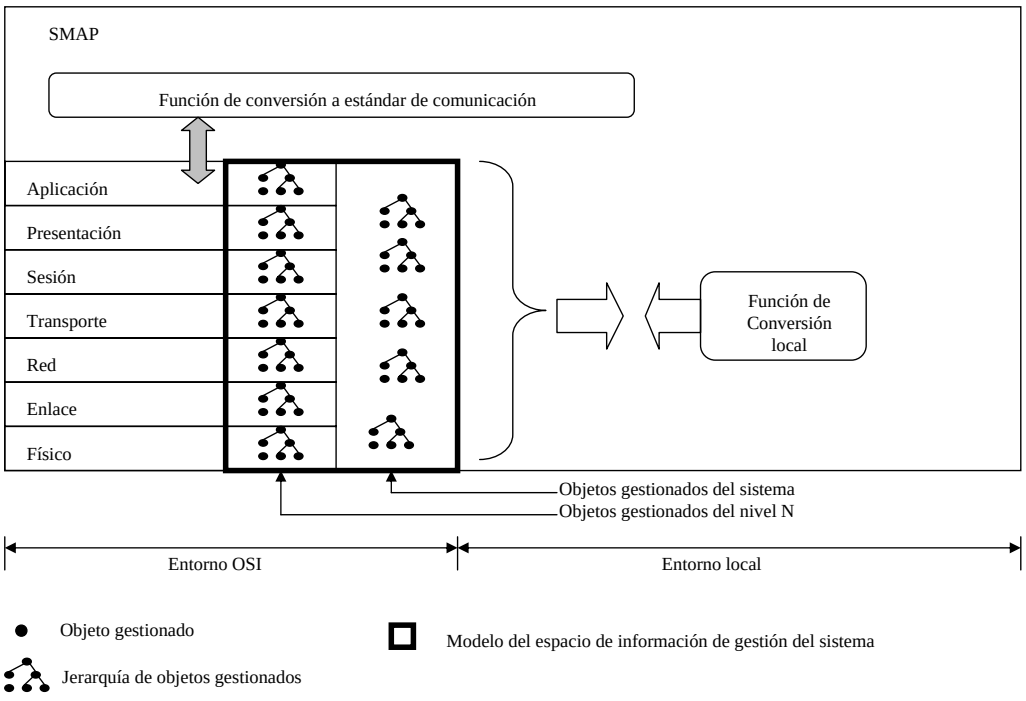
- Todos los elementos descritos deben existir en cada uno de los elementos a gestionar en el sistema (red).
- El SMAP puede tomar el papel de **agente** o de **gestor**. El papel de **gestor** corresponde a lo(s) centro(s) de control de red, y el de **agente** a los sistemas gestionados.
- Un **gestor** solicita información o solicita la ejecución de comandos a los sistemas gestionados. El **agente** interacciona con el **gestor** y es responsable de administrar los objetos de su sistema.



Almacenamiento de la información

- La forma de representación y almacenamiento de los datos en un agente, a partir de la cual se deriva la información de gestión no se estandariza.
- Una función local se utiliza para convertir la información relacionada con los objetos gestionados a un formato en que se pueda almacenar localmente y ser usada por el software de gestión local.
- Puesto que para que exista interacción con otros sistemas es necesaria una forma estándar de representación, otra función se encarga de realizar las conversiones necesarias.
- La información se almacena en **objetos** definidos por atributos, operaciones que se pueden realizar sobre él, notificaciones que puede emitir y sus relaciones con otros objetos (es una representación orientada a objetos).
- Los objetos representan recursos, y las operaciones se realizan sobre los objetos directamente, no sobre los recursos que representan.
- Aunque un recurso soporte más operaciones, sólo aquellas definidas para el objeto correspondiente están disponibles para la gestión del sistema.

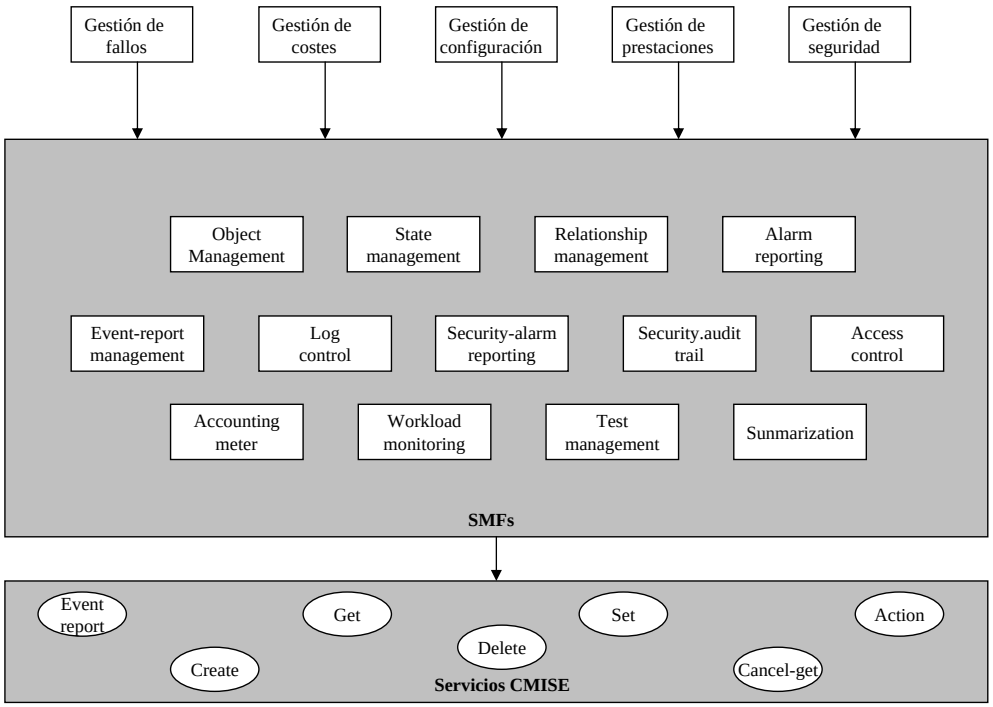
Almacenamiento de la información



Funciones de gestión de sistemas

- Las áreas funcionales de gestión (**SMFA - system-management functional area**) que define OSI son muy amplias y se definen a un nivel descriptivo. De hecho estas áreas no están estandarizadas como tales.
- Cada una de estas áreas supone el uso de funciones específicas, y hay un considerable solapamiento entre estas funciones de soporte.
- Se estandarizan un conjunto de funciones específicas, llamadas **SMFs (*system management functions*).** Cada estándar de SMF define la funcionalidad para soportar los requisitos de las SMFAs. Una SMF determinada puede dar soporte a varias SMFAs y cada SMFA requiere varias SMFs.
- Cada estándar de SMF define su funcionalidad y proporciona una correspondencia entre los servicios de la SMF y de la CMISE. Cada SMF puede utilizar los servicios de otras SMFs y de la CMISE.

Funciones de gestión de sistemas



Funciones de gestión de sistemas

- Están estandarizadas 13 SMFs:
  - ***Object management***: soporta la creación y borrado de objetos gestionados y la lectura y cambio de atributos de objetos. También especifica las notificaciones que se deben enviar cuando cambia el valor de un atributo.
  - ***State management***: especifica el modelo de representación del estado de gestión de un objeto. Proporciona servicios para soportar ese modelo.
  - ***Relationship management***: especifica el modelo de representación y gestión de relaciones entre objetos. Proporciona servicios para soportar ese modelo.
  - ***Alarm reporting***: soporta la definición de alarmas de fallos y las notificaciones utilizadas para comunicarlas.
  - ***Event-report management***: soporta el control de informe de eventos (notificaciones), incluyendo la especificación de los receptores de la notificación, la definición de notificaciones, y la especificación de criterios para generar y distribuir notificaciones.

Funciones de gestión de sistemas

  - ***Log control***: soporta la creación de históricos, la creación y almacenamiento de registros en históricos, y la especificación de criterios para realizar históricos.
  - ***Security-alarm reporting***: soporta la definición de alarmas de seguridad y las notificaciones utilizadas para comunicarlas.
  - ***Security-audit trail***: especifica los tipos de informe de eventos que debería contener un histórico utilizado para evaluación de seguridad.
  - ***Access control***: soporta el control de acceso a la información y operaciones de gestión.
  - ***Accounting meter***: proporciona informes de la utilización de los recursos del sistema y un mecanismo para poner límites.
  - ***Workload monitoring***: soporta la monitorización de atributos de los objetos relacionados con las prestaciones del recurso.
  - ***Test management***: soporta la gestión de procedimientos de prueba y diagnóstico.
  - ***Summarization***: soporta la definición de medidas estadísticas para los atributos y la comunicación de la información resumida.

MIB

- El estándar ISO 10165-1 (X.720) presenta un modelo general de la MIB en sistemas OSI. En concreto:
  - Define el modelo de información de los objetos gestionados y sus atributos.
  - Define los principios para nombrar los objetos y sus atributos,de manera que puedan ser identificados y accedidos por los protocolos de gestión.
  - Define la estructura lógica de la información de gestión (SMI -*structure of management information*).
  - Describe el concepto de clases de objetos gestionados y las relaciones en las que pueden participar, incluyendo herencia, especialización, y polimorfismo.

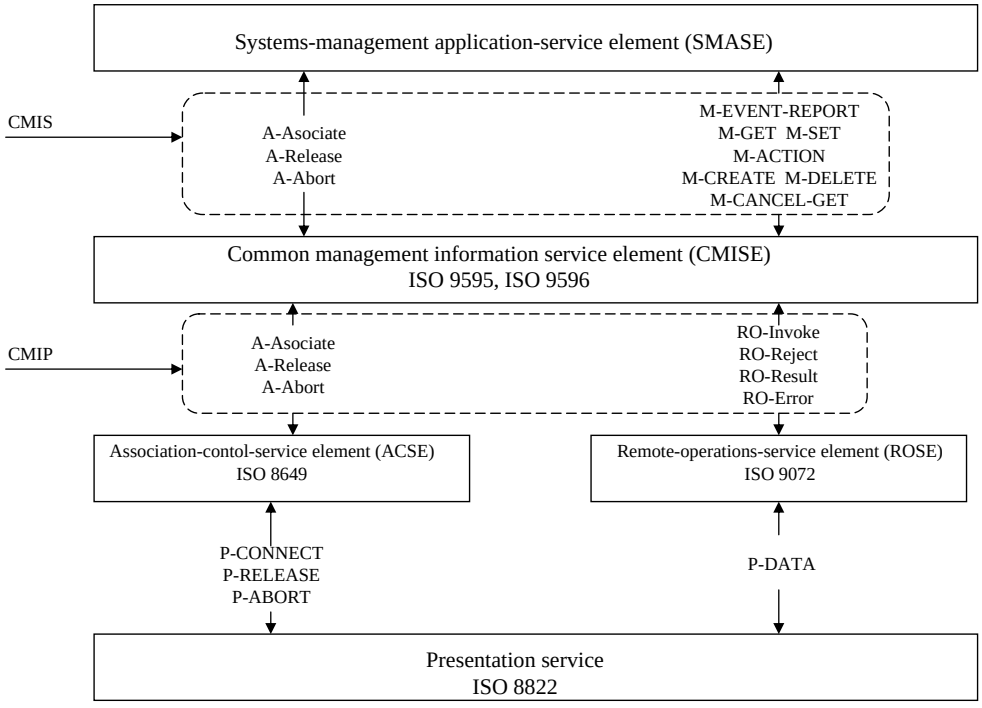
Estructura de la MIB (SMI)

- Está definido en ASN.1.
- La unidad básica de información es el **objeto**. Un objeto puede incluir:
  - ***Atributos***: variables que representan características de los recursos gestionados
  - ***Comportamientos***: acciones que pueden ser disparadas por un **gestor**.
  - ***Notificaciones***: informe de eventos que pueden ser disparados por determinados eventos.
- La definición ASN.1 sigue el formato de **clases de objetos**. Para cada clase, la información actual se representa mediante **instancias de objeto**. Es decir, puede haber varias instancias de un objeto para una determinada clase, cada una con valores de atributos diferentes.
- Existen dos formas de crear jerarquías para estructurar la MIB:
  - Definición de subclases, o clases derivadas de otras clases que heredan sus características.
  - Una instancia de objeto puede estar contenida en otra instancia de objeto.

Protocolo (CMIS/CMIP)

- El intercambio de información entre dos entidades (**gestor**, **agente**) es una de las funciones básicas del sistema de gestión OSI. Esta función de intercambio de información en el sistema de gestión OSI se conoce como CMISE (*common management information service element*). Como la mayoría de las áreas de funcionalidad en OSI, CMISE se especifica en dos partes:
  - La interfaz con el usuario, especificando los servicios proporcionados. Se denomina CMIS (*common management information service*).
  - El protocolo, especificando el formato de las PDUs (*packet data unit*) y los procedimientos asociados. Se denomina CMIP (*common management information protocol*).
- El CMIS proporciona 7 servicios para realizar operaciones de gestión mediante primitivas de servicio. Además los usuarios necesitan establecer asociaciones entre CMISEs para poder realizar operaciones de gestión. Para ello existen 3 primitivas que proporciona el ACSE (*association-control-service element*) y que pasan de manera transparente el CMISE.
- Para los servicios de gestión el CMISE emplea el CMIP para intercambiar PDUs, para los servicios de asociación, no interviene el CMIP.

Protocolo (CMIS/CMIP)



Protocolo (CMIS/CMIP)

- Primitivas de servicio CMIS:
  - *M-EVENT-REPORT*: usado por un agente para notificar la ocurrencia de un evento a un **gestor**.
  - *M-GET*: Usado por un **gestor** para obtener información de un **agente**.
  - *M-SET*: Usado por un **gestor** para modificar información de un **agente**.
  - *M-ACTION*: Usado por un **gestor** para invocar un procedimiento predefinido especificado como parte de un objeto de un **agente**. La petición indica el tipo de acción y los parámetros de entrada.
  - *M-CREATE*: Usado para crear una nueva instancia de una clase de objetos.
  - *M-DELETE*: Usado para eliminar uno o más objetos.
  - *M-CANCEL-GET*: Usado para finalizar una operación *GET* larga.
- No vamos a ver las PDUs del CMIP. Las primitivas de servicio de CMIS se convierten en las correspondientes PDUs que utilizan los los servicios del ASCE, del ROSE y del servicio de presentación.